UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
BROWNSVILLE DIVISION

UNITED STATES OF AMERICA	§	
	§	
VS.	§	Case No.: 1:19-cr-00601-1
	§	
ALVARO VEGA-RODRIGUEZ	§	

FIRST SUPPLEMENTAL MOTION TO SUPPRESS EVIDENCE

Now comes the Defendant, **ALVARO VEGA RODRIGUEZ** by and through his attorneys of record, **ERNESTO GAMEZ, JR., ERIN E. GAMEZ, of The Law Offices of Ernesto Gamez, Jr., P.C.,** moves the court to suppress all evidence, materials and statements obtained from the unlawful search, detention, and interrogation on or about June 4, 2019, by the Department of Homeland Security Investigations and the Brownsville Police Department and/or any law enforcement officer, on the following grounds:

I.

After discovery of file, extensive research, and multiple meetings with the U.S. Attorney's office and federal agents in an attempt to resolve the issues, Defendant, by and through counsel, and for good cause would show and hereby request the Court to look into potential privileged Fourth Amendment violations occurring in Cameron County and potentially other areas of the State of Texas from the use by Federal Agents of highly technological, digital, hash value computer equipment which use potentially circumvents the legal requirement of first requesting a search warrant.

II.

According to the Reports of Investigation (hereinafter, "R.O.I.") provided by the Assistant United States Attorney's Office, the case against Mr. Vega-Rodriguez commenced on or about May 5, 2019 while Government Homeland Security agents were conducting a *warrantless* "online investigation," using "investigative BitTorrent software." From the limited evidence provided in this case, it is apparent that Government agents, utilizing "investigative BitTorrent software," were working directly with the hash value identifiers stored in the National Center for Missing and Exploited Children (hereinafter, "NCMEC") database. (From the evidence provided by the Government, it is clear this case did not involve a third-party tip to agents from an electronic service provider, or anyone else.) To date, after multiple formal and informal discovery requests from the Defendant, the Government has failed to provide all of the following, but not limited to: the defense access to the "investigative BitTorrent software", any documentation or paperwork identifying the purported "investigative," software utilized by the Government in this case (or how the software works), the software license agreement for the "investigative" software, the user handbook or guidelines for the "investigative" software, any agreement with BitTorrent allowing them to utilize this "investigative" software on the BitTorrent platform, the date and time stamped downloaded files in this case, the date and time stamped trajectory of the downloads utilized in this case, the government's internet protocol address utilized in this case, the search terms utilized in this investigation, among many other material, relevant evidence utilized in this vaguely summarized "online investigation." In short, the defense has been relegated to defend these extreme accusations with vague summaries identified in Government agents' R.O.I.'s and the purported end result of photos of contraband.

Nearly one month after the "online investigation," law enforcement agencies, on or about

June 4, 2019, forcefully entered the Defendant's homestead on or before 6:00 a.m., ordered all occupants out of the home and onto the front lawn, handcuffed and detained the Defendant, and began interrogating the Defendant, without validly Mirandizing the Defendant and affording him of his rights. This unlawful interrogation without the Defendant's knowing, voluntary consent and waiver, resulted in the search and seizure of the computer passwords, access codes, laptop computers, files and other admissions against the Defendant's interests.

During the interrogation of Defendant at his homestead any and all statements and admissions excised from the Defendant were made prior to the execution of any such waiver by the Defendant of the rights afforded to him by the Fourth, Fifth, Sixth and Fourteenth Amendments to the United States Constitution. Any and all statements made by the Defendant, and fruits of those statements, were not validly secured as they were not the product of a voluntary, a knowing, and intelligent relinquishment of such rights.

III.

The search and seizure of materials and statements therefrom on the occasion in question violated the rights of this Defendant under the First, Fourth, Fifth, Sixth, Ninth and Fourteenth Amendments to the United States Constitution and under Article I, Sections 9, 10 and 19 of the Texas Constitution.

IV.

The Defendant moves the court to suppress the following evidence:

a. All files, photos, downloads, electronic evidence and such other evidence produced as a result of the Government's "online investigation," utilizing "investigative BitTorrent software;"

b. All statements made, whether written or oral, and such other actions of this defendant, which occurred at or subsequent to his/her detention on or about June 4, 2019;

c. All books, letters, notes, records, documents and other tangible things that were seized from the Defendant on or about June 4, 2019; and

d. The testimony of any law enforcement officers, agents and all other persons working in connection with such officers and agents, and all persons present at or near the location of the arrest of the Defendant and the search of his residence in regard to any statements or evidence acquired or objects seized as set forth in paragraph "I" above.

V.

Defendant would show the court the following legal objections:

a. The arrest of the Defendant was made based on a warrant premised almost entirely on hearsay, which misrepresented probable cause, and in violation of his rights under the Fourth, Fifth and Fourteenth Amendments of the United States Constitution. *Beck v. Ohio*, 85 S.Ct. 223, 379 U.S. 89, 13 L.Ed.2d 142 (1964); *Payton V. New York*, 100 S.Ct. 1371, 445 U.S. 573, L.Ed.2d 639 (1980).

b. All statements made by the Defendant at the time of and subsequent to his detention were products of his illegal arrest. *Dunnaway v. New York*, 99 S.Ct. 2248, 442 U.S. 200 60 L.Ed.2d 824 (1979); *Wong Sun v. United States*, 371 U.S. 471, 83 S.Ct. 407, 9 L.Ed.2d 441 (1963); Fourth, Fifth and Fourteenth Amendments, United States Constitution.

c. Any statement made by the Defendant was not freely nor voluntarily made but was given as a result of compulsion and/or persuasion. *Jackson v. Denno*, 378 U.S. 368, 84 S.Ct. 1774, 12 L.Ed. 2d 908 (1964); *Miranda v. Arizona*, 384 U.S.

436, 86 S.Ct. 1602, 16 L.Ed. 2d 694 (1966); Fifth and Fourteenth Amendments, United States Constitution.

d. Statements given by the Defendant were made as a result of an interrogation that occurred when the Defendant did not have advice of counsel, wherein he had not been warned of his right to invoke his right to counsel, in violation of the rights guaranteed to him by the Fifth, Sixth and Fourteenth Amendments, United States Constitution. Edwards v. Arizona, 451 U.S. 477, 101 S.Ct. 1880, 68 L.Ed. 2d 378 (1981).

e. That any alleged waivers by the Defendant of rights secured to him under the Fourth, Fifth, Sixth and Fourteenth Amendments to the United States Constitution were not valid because they were not voluntary and/or not a knowing and intelligent relinquishment of such rights. *Johnson v. Zerbst*, 304 U.S. 458, 58 S.Ct. 1019, 82 L.Ed. 1461 (1938); *Schneckloth v. Bustamonte*, 412 U.S. 218, 93 S.Ct. 2041, 36 L.Ed. 2d 854 (1973); *Edwards v. Arizona*, 451 U.S. 477, 101 S.Ct. 1880, 68 L.Ed. 2d 378 (1981); *Michigan v. Jackson*, 106 S.Ct. 1404 (1986).

f. That the search of the Defendant's home was without a warrant and without probable cause and any consent to search was not voluntary. *Coolidge v. New Hampshire*, 403 U.S. 443, 91 S.Ct. 2022, 29 L.Ed. 2d 564 (1971); *Schneckloth v. Bustamonti*, 412 U.S. 218, 93 S.Ct. 2014, 36 L.Ed. 2d 854 (1973); *Bumper v. North Carolina*, 391 U.S. 543, 88 S.Ct.1788, 20 L.Ed. 2d 797 (1968).

g. For such other and further reasons as may appear or exist upon a full evidentiary hearing of this cause.

VI.

The product of such search and seizure is therefore unlawful and all fruits thereof must be suppressed. All statements, either written or orally made, and all materials and substances seized during and after such acts were fruits of the initial violation of rights of this Defendant.

"2015 Potential Fourth Amendment violations of Microsoft Blood PhotoDNA data donated to the" National Center for Missing and Exploited Children (NCMEC) for all issues related to the prevention of and recovery from, child victimization, include abduction, abuse and exploitation.

VII.

After discovery of governments file, extensive research, and multiple meetings with the U.S. Attorney's office and federal agents in an attempt to resolve the issues, Defendant, by and through counsel, and for good cause would show and hereby request the Court to look into potential privileged Fourth Amendment violations occurring in Cameron County and potentially other areas of the State of Texas from the use by Federal Agents of highly technological, digital, hash value computer equipment which use potentially circumvents the legal requirement of first requesting a search warrant.

XIII.

The scenario where an undercover agent/person is approached by an individual with a computer for child porn photographs and is a thing of the past.

Federal agents are now able to invade, intrude, encroach, infringe, and trespass into anyone's computer used in the privacy of their own home by the use of Microsoft photo DNA.

Microsoft© -created a PhotoDNA-data software which develops an actual digital fingerprint of a child's photograph similar to an ID fingerprint of a person, a/k/a **"Hash Value."**

1. Microsoft© created a **Hash Value** of each photo of each child photo to assist the government in identifying children similar to the individual fingerprint of persons.
2. These known or identified hash values are then stored in the NCMEC database to assist electronic service providers (a third party) and Government agents in identifying online child contraband.
3. Federal Agents purportedly place these known, stored, monitored hash values in their Homeland Security Investigations (hereinafter HSI) office computer "investigative" software during Homeland Security Investigations.
4. Federal Agents now are able to literally determine a person's private computer contents if they possess a Hash Values child photo DNA.
5. HSI office computers are a dictionary of these Hash Value child photos. The Federal Agents then simply check an Internet Protocol (IP) address. The (IP) informs Agents the location of home and computer which possess child photo DNA Hash Value.
6. Thus, Homeland Security agents are in actuality able to search your computer, seize and identify Hash Value information that micro photo DNA, and locate the residence, without first seeking a search warrant. In other words, Agents are in without a search warrant.

In reality agents searched, identify information, circumventing a warrant, and later say they have reason to believe or probable cause exists for a search warrant, when in fact, Federal Agents have already searched, found and located Microsoft photo DNA child from private computer by

use of their Homeland Security Investigations office computer without first going to a magistrate for a warrant.

IX.

Agents for the government then artfully craft an affidavit for the court without specificity as to how, or without informing the Court that:

(1) they have already intruded into a person's computer without a search warrant.

(2) That they already identified hash value DNA photos from a private computer without a search warrant;

(3) that the government already entered the defendant's home, entered into his bedroom, and entered into his computer, all without a search warrant, by use of (HST) Aka "Hash Values" in photo child DNA photos.

(4) In this case the person can log into an app titled as "Caldo de Pollo" and unknowingly connect and attach therein 1000 child porn photos. The individual may have only checked and looked at one or maybe less than 20 and stopped looking, but is charged with the possession of 1000 child porn photos, simply due to the government possessing one hash value child from DNA photograph being attached to the particular app containing 1000 child porn photos.

(5) The defendant may or may not know that what he was accessing is 1000 porn photos and he was trapped, is now charged with possessing 1000 porn, photos and elevated to 6 base level points under the Federal Sentencing Guidelines.

(6) This is even in the government, cannot prove that Defendant personally looked into 1 or 100, or 1000 child porn photos.

Defendant respectfully that these child porn photographs be suppressed as violating the Fourth amendment of the United States.

X.

The Tenth Circuit has identified NCMEC, although ostensibly a private corporation, to be both a governmental entity and a government agent. See, *United States v. Ackerman*, 831 F.3d 1292 (10th Cir., August 5, 2016.) More importantly, the *Ackerman* Court determined that, in that instance where a third party (electronic service provider) tip was not involved, NCMEC's participation in the search was also that of a governmental law enforcement agency and, therefore, implicated the fourth amendment. See, *Id*. However, the United States District Court, District of Vermont, determined that where a third-party electronic service provider initiates the search and merely passes that information along to NCMEC and/or law enforcement agency in the form of a tip, that does not trigger the fourth amendment consequences. See, *United States v. Coyne,* 387 F.Supp.3d 387 (D., Vt. 2018.) Unlike the third-party tip in *Coyne*, the facts in this case implicate a direct search by Government HIS agents with assistance from NCMEC, more similar to the *Ackerman* case.

In this case, the R.O.I.s merely explain that Government task force agents were conducting a vague "online investigation" of a specific geographic area without any evidence that there was *probable cause* to launch said "investigative BitTorrent software," in the geographic area. The R.O.I.'s provided in this case do not identify any particular reason or probable cause for the Government to have launched said, "investigative BitTorrent software," in this geographic area. Government task force agents were utilizing this secretive "investigative BitTorrent software," with the cooperation of NCMEC, and no other third-party tip, to allegedly tactically isolate computers and conduct a download / transaction targeting the Defendant. To date, the Government

has failed to produce any documentation whatsoever to explain, identify, or demonstrate the purported "investigative BitTorrent software," which led to the Defendant's computer, all of which is extremely material to the defense of this matter.

While the Government has provided the defense with no physical evidence identifying or explaining this purported secretive, "investigative BitTorrent software," the defense can only liken[1] it to the Government's use of a thermal imaging device, a tactic which the Supreme Court has long since deemed an unreasonable search absent a warrant. See, *United States v. Kyllo*, 553 U.S. 27 (2001) (holding that the use of a device by the government, which is not generally used by the public, to obtain evidence from inside a home is a presumptively unreasonable search.). In light of the secrecy of the "investigative BitTorrent software," the defense could also liken its usage to that of a warrantless use of a Stingray device or cell-cite simulator. See, *United States v. Lambis*, 197 F.Supp. 3d 606 (S.D.N.Y. 2016) (holding that the warrantless use by DEA agents of a cell-site simulator, to locate defendant's apartment as the place of use for the target cell phone, for which cell phone the agents had already obtained a warrant for cell site location information (CSLI), was an unreasonable search under the Fourth Amendment.) In light of the secrecy of the Government's purported "investigative BitTorrent software," and NCMEC assistance, combined with the lack of probable cause to deploy such technology, the defendant could further liken this to a warrantless homestead "knock and talk" with a drug sniffing canine on one's front porch, which the Supreme Court has also long since ruled an unconstitutional violation of the Fourth

[11] The Government has contended this "investigative BitTorrent software," can be likened to a state police agency radar gun on the highway. If this in fact were such a case, the defense would be entitled to have the Court order the policing agency to produce the radar gun used in the traffic stop for independent inspection and testing by the defense as it is a material tool involved in the probable cause for the stop. Furthermore, this analogy fails because this incident did not occur on a public highway, it allegedly occurred on a constitutionally protected device in the defendant's home. Lastly, a radar gun is not a tactical tool generally available for public use in a search of one's home.

Amendment. See, *Florida v. Jardines*, 569 U.S. 1 (2013) (holding that even though the detectives may have also smelled marijuana, the warrantless use of a drug sniffing canine at the residence allowed officers to unconstitutionally glean information from inside the home.)

The evidence this case is clear that other members of the public, along with other general users of the BitTorrent platform, do not have access to utilize the Government's "investigative BitTorrent software," in combination with NCMEC's database. While Government agents are generally allowed to interact with the public or attempt to speak with occupants of homes, when their actions or the technology they employ allows the agent to go inside the home, the search may be unconstitutional. See, *People v. Henderson*, 220 Cal. App. 3d 1632 (1990) (holding that an agent cannot use audio equipment to hear what the unaided ear cannot.); *United States v. Kim*, 415 F.Supp. 1252 (D. Hawaii 1976) (holding that police use of a telescope from a quarter mile away to view what suspect was reading was an unconstitutional search of his home.).

At the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion. U.S. Const. Amend. 4. The Fourth Amendment focuses on eliminating first and foremost, the Government's use of warrantless unreasonable *searches*, not just seizures. In this case, the Government has shrouded in secrecy their tactical, targeted use of "investigative BitTorrent software," in combination with the NCMEC database on Defendant's computer. To date, no physical information or evidence has been provided to the defense to confront this material, relevant use of government technology involved in the purported incrimination of the Defendant's computer. The defense can only be certain that this case did not involve a third-party reliable tip, nor was a warrant requested prior to deploying this secretive technology. For all the aforementioned factual information and lawful precedent

articulated herein, the Government's warrantless use of this technology should be deemed unreasonable and the fruits thereafter should be suppressed.

PRAYER

WHEREFORE, PREMISES CONSIDERED, Defendant prays that upon **hearing**, this motion be granted and that the evidence referred to herein be in all things suppressed and the United States Government and its witnesses be ordered not to disclose to the Jury or Court or in any way to allude to the fact of any materials or statement obtained thereby.

Respectfully submitted,

LAW OFFICES OF
ERNESTO GAMEZ, JR., P.C.
Justice for All Building
777 East Harrison Street, First Floor
Brownsville, Texas 78520
Telephone No.: (956) 541-3820
Facsimile No.: (956) 541-7694
E-Mail: ernestogamezjr@gamezlawoffices.com

BY: */s/ Erin Elizabeth Gamez*
ERIN ELIZABETH GAMEZ
State Bar No. 24093469
Federal Id. No. 2627599

ERNESTO GAMEZ, JR.
State Bar No. 07606600
Federal Id. No. 8645

ATTORNEYS FOR DEFENDANT
ALVARO VEGA-RODRIGUEZ

CERTIFICATE OF CONFERENCE

I, **ERIN ELIZABETH GAMEZ**, hereby certify that on this **31st day of December 2019**, I conferred with the opposing counsel, **Hon. Joe Esquivel**, United States Assistant Attorney, regarding the filing of this motion, and hereby state that he is opposed to this motion.

/s/ Erin Elizabeth Gamez
ERIN ELIZABETH GAMEZ

CERTIFICATE OF SERVICE

I, **ERIN ELIZABETH GAMEZ**, do hereby certify that on this 31st **day of December 2019**, **a** true and correct copy of the above and foregoing **First Supplemental Motion to Suppress Evidence** and its **Order** were served **electronically** upon **Ms. Ana Cecilia Cano**, Assistant United States Attorney, **United States Attorney's Office**, 600 East Harrison Street, Suite 201, Brownsville, Texas, 78520, ana.cano@usdoj.gov.

/s/ Erin Elizabeth Gamez
ERIN ELIZABETH GAMEZ